Machine Learning in Cyber Security Response and Automation

University of Strathclyde
Dept. of Electronic and Electrical Engineering
Institute of Sensors, Signals and Communications

Robert Atkinson, Christos Tachtatzis, Xavier Bellekens,
Ivan Andonovic

Objectives

University of Strathclyde Engineering

- Highlight Cyber Threats to Critical Infrastructure and Governmental Organisations
- Identify and Demonstrate Cyber Threat Detection in Complex Environments
- Establish why AI and ML is apprpriate for autonomous vulnerable host detection
- Present a Cyber Framework for Autonomous Cyber Response

Cyber Threat Landscape

University of Strathclyde Engineering

- Targeted Attacks
  - 0-Days
- Increased Disruption
  - Internet outage
- Distortion
  - Mis-information
  - Falsified Information
- Deterioration
  - Legacy Systems

Home Owner Threat Landscape

University of Strathclyde Engineering

- Sensitive IoT information
- Listening Home Assistants
- Vulnerable Connected Devices
  - Routers
  - Cameras
  - Babyphones
  - Dolls

Critical Infrastructure Threat Landscape

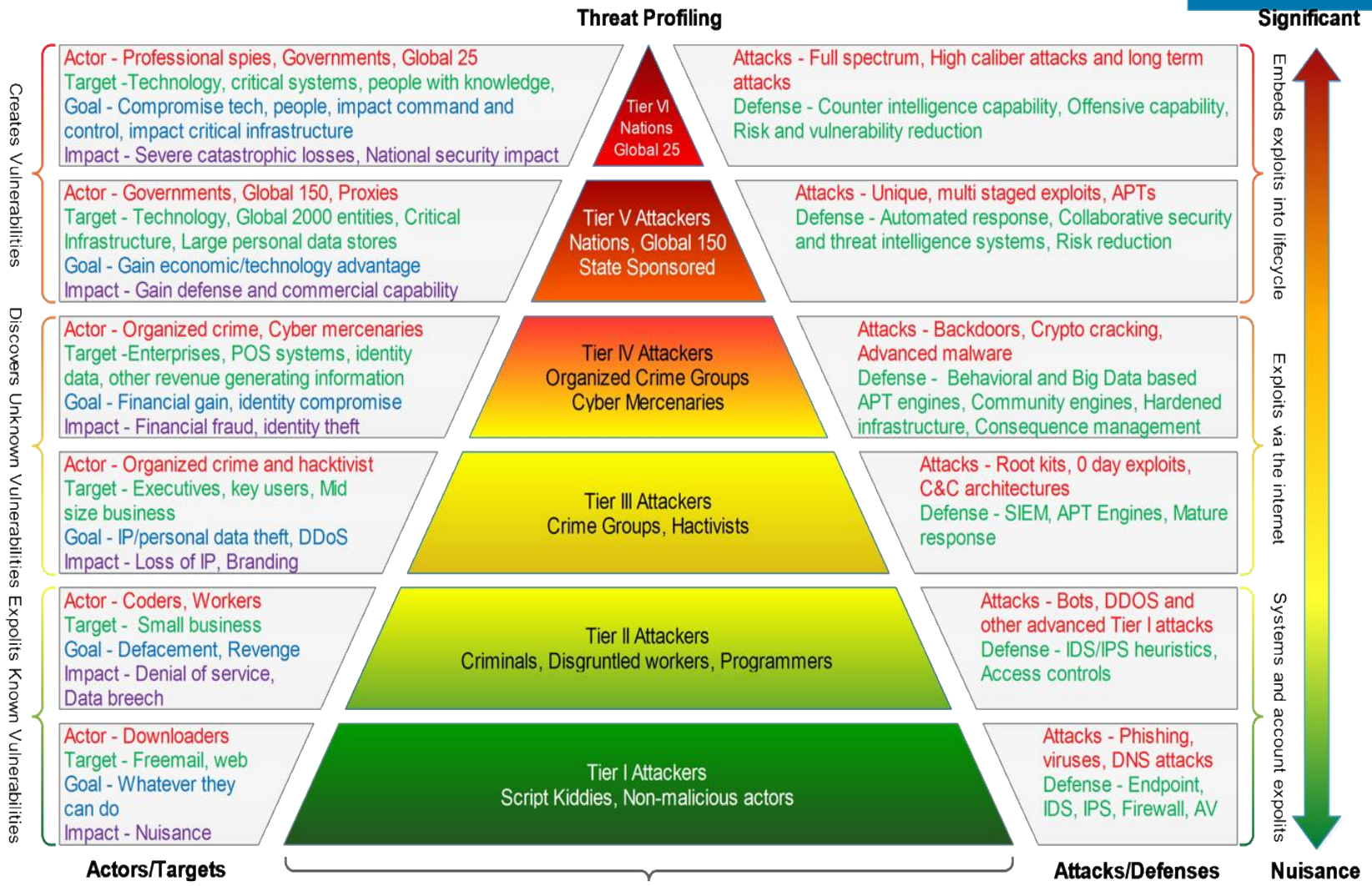
University of Strathclyde Engineering

- Targeted Attacks
- Supply Chain Infiltration
- Legacy Systems
- SCADA Systems
- Crypto-mining Malwares (2018 – Water Infrastructures)

Governmental Threat Landscape

- Cyber Espionage
- Public Misinformation
- Foreign Governments Interference
- Cyber Physical Attacks[1]
  - Energy
  - Transport
  - Banking
  - Financial Markets
  - Health
  - Water Supply
  - Digital Infrastructure

[1] DIRECTIVE (EU) 2016/1148



https://www.recordedfuture.com/prioritizing-cyber-threats/

Complex Networks

University of Strathclyde Engineering

- Heterogeneous Networks
- Distributed Networks
- Internet of Things (IoT)
  - ➢ Physical Implications

Machine Learning

University of Strathclyde Engineering

- Blue Team (Reactive)
  - Network Anomaly Detection
  - Intrusion Detection Systems
  - User Behaviour
  - Identify misinformation – Government interference and Fake News
- Red Team (Proactive)
  - Vulnerable Host Identification
  - Automated Cyber Response

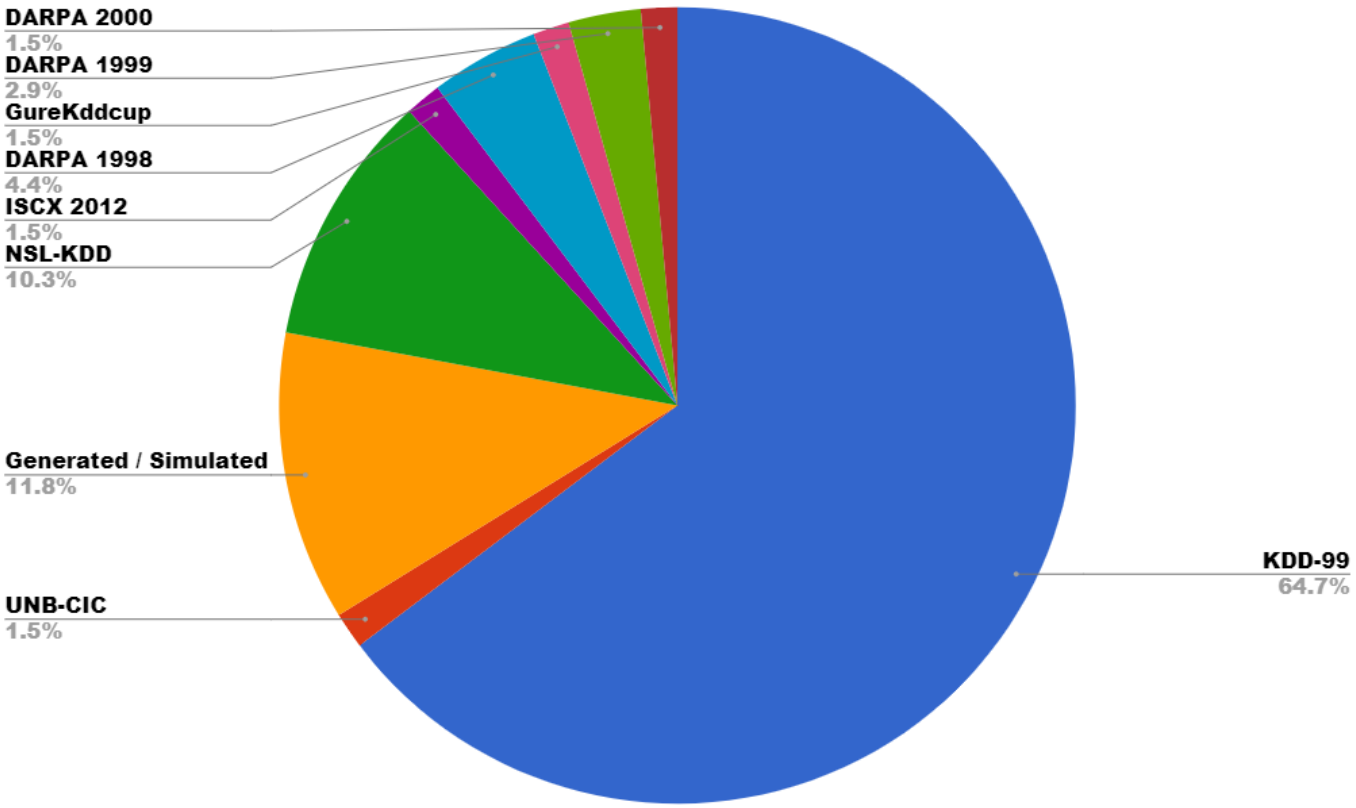
Data Challenge

University of Strathclyde Engineering

- Clarify Objectives
- Collect Appropriate Data
- All data is manipulated data[1]
- Create Synthetic & Real Representative Datasets
- Datasets must be flexible

[1] Angela Bassa, 2019

Current Intrusion Detection Datasets



Hindy, H., et al. "A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets. arXiv 2018." arXiv preprint arXiv:1806.03517.

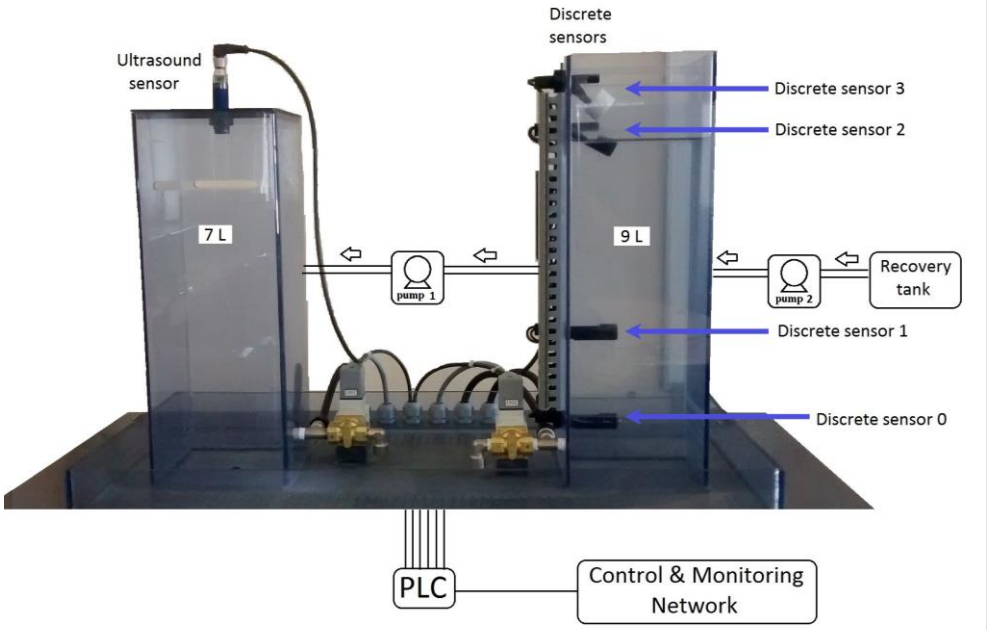
Intrusion Detection Systems (Blue Team)

University of Strathclyde Engineering

- Detect Attacks against SCADA Networks
- Improve Security information and event management (SIEM)
- Detect 0-Day attacks

Water Supply Intrusion Detection Systems

- Accurately detect Attacks against
  - The SCADA Network
  - The Sensors
- Provide Key Information to the Operator on the type attacks
  - Cyber Attack
  - Breakdown (Predictive Modeling)
  - Sabotage
  - Potential Hits to the Tank



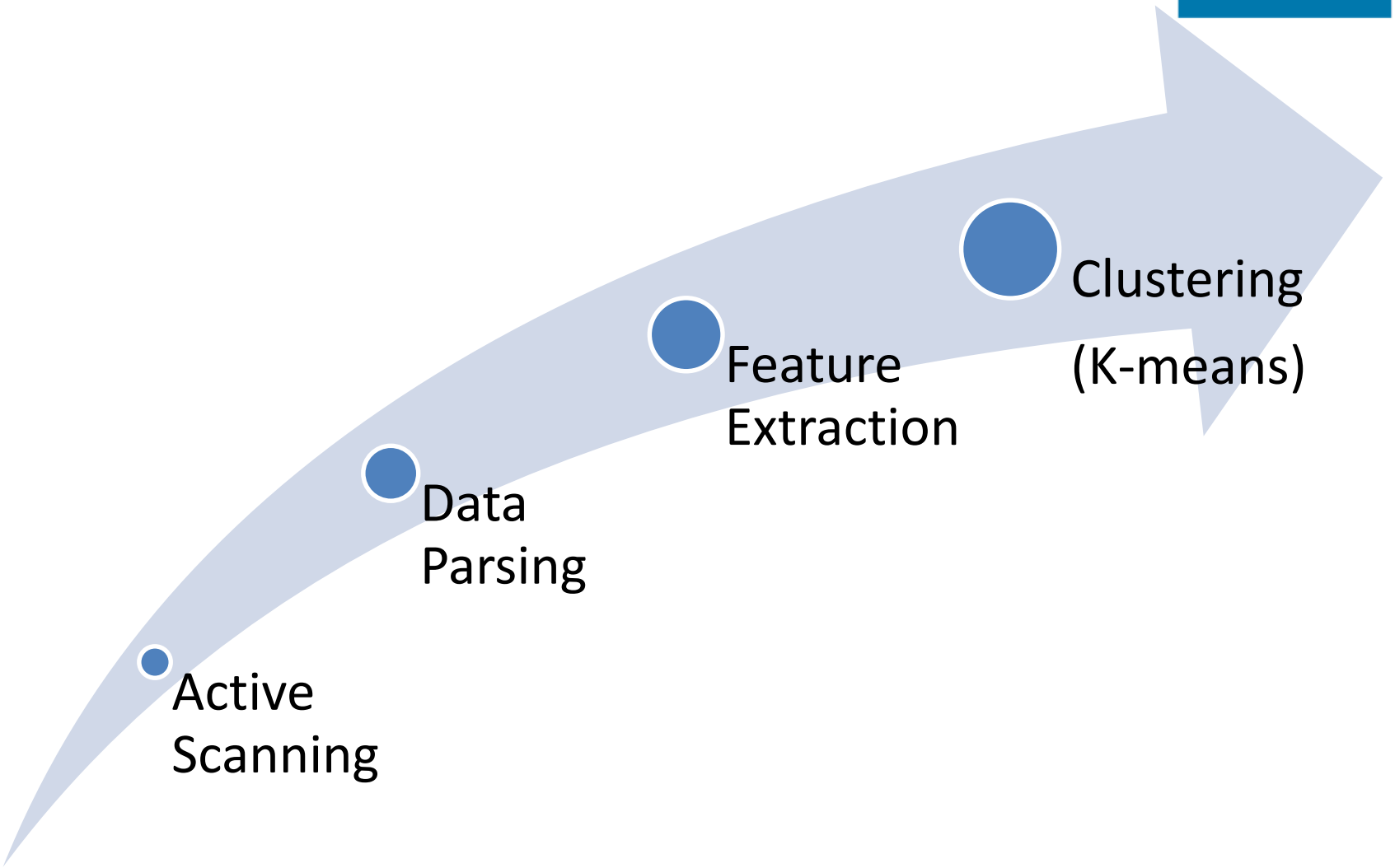
Vulnerable Hosts Identification (Red Team)

University of Strathclyde Engineering

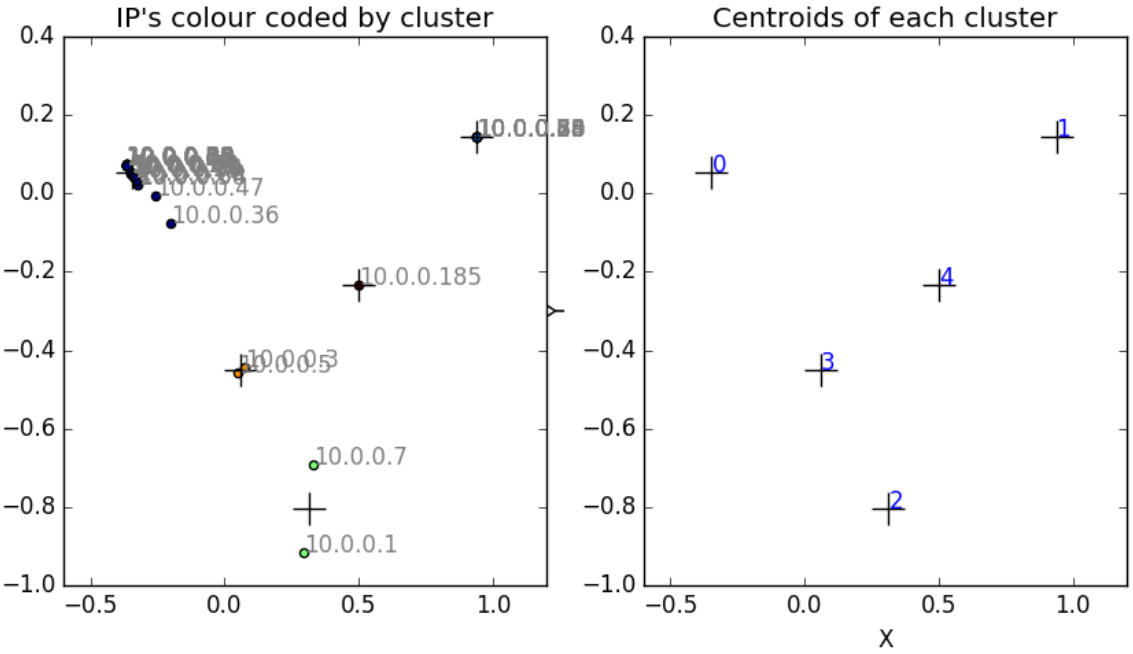
- Penetration testing of large corporate network
  - Expensive
  - Time consuming
  - Analysing results
  - Vulnerable hosts identification
- Automated exploitation (e.g. Metasploit)
  - Time consuming
- Automated Vulnerability Scanner
  - Inconvenient Output (With Large Network)

Vulnerable Hosts Identification

University of Strathclyde Engineering

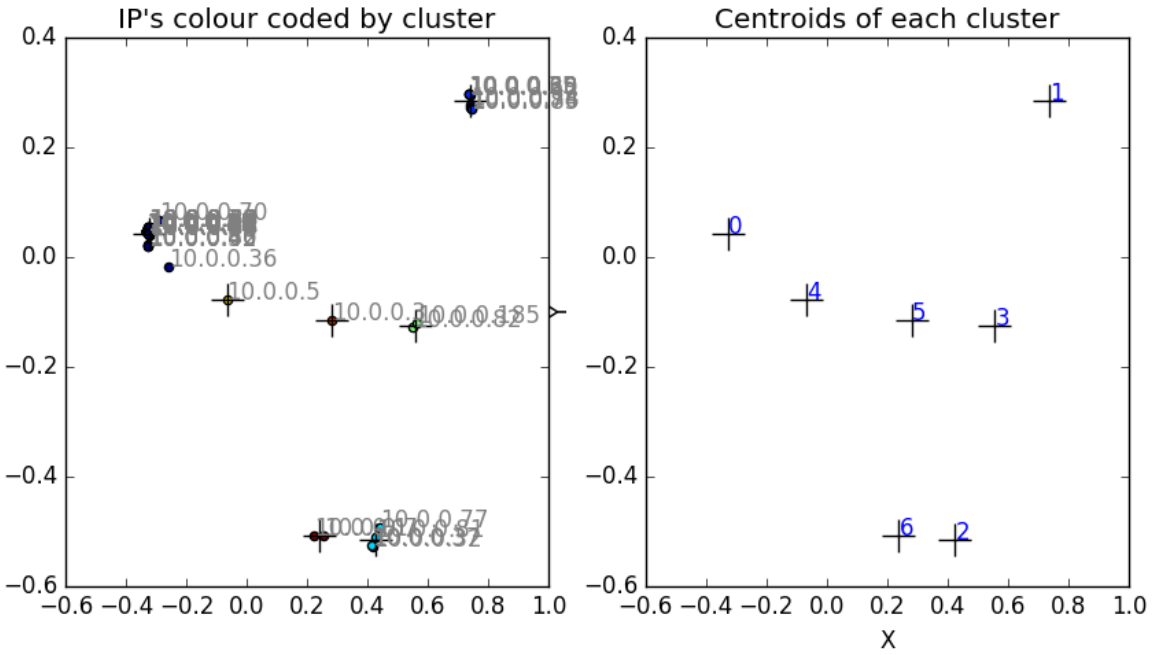


Vulnerable Hosts Identification (Nmap)



Vulnerable Hosts Identification (Nessus)

University of Strathclyde Engineering



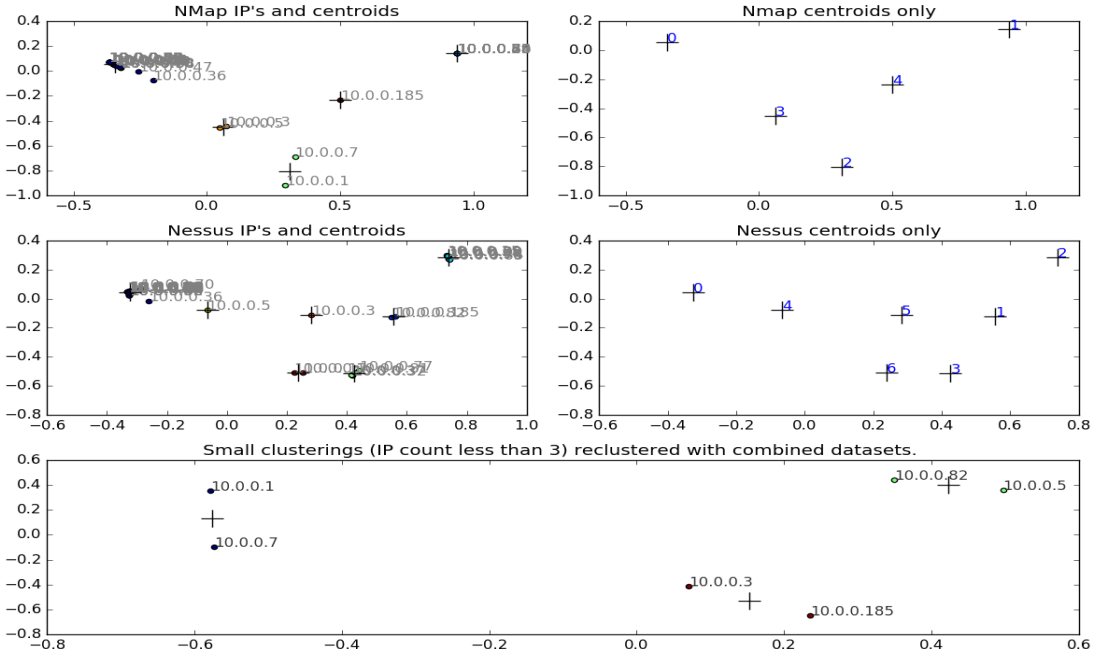
Vulnerable Hosts Identification (Combined)

University of Strathclyde Engineering

Recommendations provided

10.0.0.5 : Windows 7 SP0
10.0.0.7 HP iLO 2
10.0.0.185. Linux 3.11 Kernel

All these hosts contain a vulnerability and are exploitable



Recommended attack vectors:
10.0.0.5 : "Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8. Prediction accuracy: 100"
10.0.0.7 : "HP iLO 2 remote management interface. Prediction accuracy: 100"
10.0.0.185 : "Linux 3.11 - 3.14. Prediction accuracy: 100"
10.0.0.1 : "Linux 2.6.18 - 2.6.22. Prediction accuracy: 86"
10.0.0.3 : "Linux 3.11 - 3.14. Prediction accuracy: 100"

Vulnerable Hosts Identification

University of Strathclyde Engineering

- Clusters
  - Vulnerable hosts (Same Vulnerability)
  - Non-Vulnerable Hosts
  - Outliers
- Targeted Attacks
  - Identify outliers (printers, servers, etc)
- Accurately identify infected hosts
  - Malware
  - Crypto-miners
  - Etc..

Autonomous Cyber Response

University of Strathclyde Engineering

- Offensive Cyber Security
  - Deterrent: Integral part of the military power

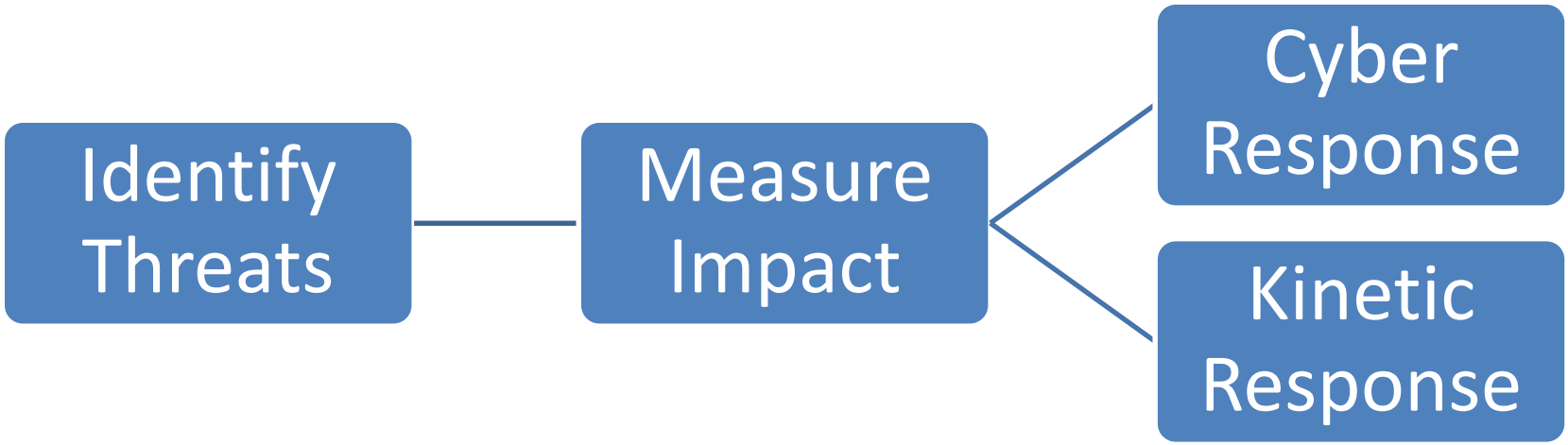
Autonomous Cyber Response (Blue Team)

University of Strathclyde Engineering

- Anticipate Threats
- Autonomously Detect Incidents (Internal and Externals)
- Reduced Escalation & Automated Recovery (Moving Target Defense)
- Automated Incident Investigation and Triage (Digital Forensics)

Autonomous Cyber Response (Red Team)

University of Strathclyde Engineering



Human in the Loop: Critical Thinking Factors[1]

University of Strathclyde Engineering

- NATO Article 5 is the backbone of our collective defence
  - ➢ Sufficiently vague for the selection of the level of deterrent (avoiding cyber attacks under a threshold)

1 Caton, Jeffrey L. "Exploring the prudent limits of automated cyber attack." 2013 5th International Conference on Cyber Conflict (CYCON 2013). IEEE, 2013.

Kinetic Response

Israel Defense Forces
@IDF

CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work.

HamasCyberHQ.exe has been removed.

♡ 5,402 4:55 PM - May 5, 2019

May 12, 2019 | *Topic:* Security | *Blog Brand:* The Buzz | *Tags:* Israel, Cyber Warfare, War, Gaza, Hamas

Israel Bombed Cyber Hackers (That Is Historic, For Many Reasons)

Should nation-states start kinetic conflicts over cyber battles?

THE NATIONAL INTEREST

Autonomous Cyber Response (Red Team)

University of Strathclyde Engineering

- Training is central (Cyber Range – H2020 FORESIGHT Project Starting in September 2019 – 22 Partners)

  - Advanced Threat Detection
  - Data Analytics Capabilities
  - Attack Attribution
  - Passive and Active Information Gathering
  - Algorithmic Capabilities
  - Consequence Evaluation and Monitoring

Summary

University of Strathclyde Engineering

- Challenges of ML in Cyber Security
  - Heterogeneous Networks
  - Representative Training Data
  - Complex Threat Landscape
  - Ethical Concerns

University of Strathclyde Engineering

Questions